WHAT IS CLAIMED IS:

1. A method for enabling a user to access a restricted area via biometric authentication, the method comprising:

> receiving a portion of user information used to enable the user to access the restricted area, said information presented by a system operator;

> storing, in a database, in association with an identification code said portion of user information as a partially enabled user record;

> communicating the identification code to the user;

> receiving, at a system point of access, a record enablement request, said request including the identification code and a user biometric sample; and

> storing the user biometric sample with said user record.

2. The method of claim 1, further comprising marking said user record as active.

3. The method of claim 1, further comprising granting the user access to the restricted area.

4. The method of claim 3, wherein access to the restricted area provides access to a restricted activity.

5. The method of claim 1, wherein the enablement request further includes a user system identification number used in conjunction with the user biometric to identify the user.

6. The method of claim 1, wherein the identification code associated with the user record is chosen by the system operator.

7. The method of claim 1, wherein

8. the identification code is digitally read.

9. The method of claim 7, wherein the identification code is digitally read from a token.

10. The method of claim 7, wherein the identification code is digitally read from an electronic device.

11. The method of claim 9, wherein the identification code is a device system registration code.

12. The method of claim 1, wherein the identification code is automatically communicated to the user.

13. The method of claim 1, further comprising the system operator associating access parameters with said user record.

14. The method of claim 12, wherein the access parameters determine the manner in which the user accesses the restricted area.

15. The method of claim 12, wherein the access parameters include regulating one or more of the time the user is allowed to enable said user record, the user access frequency once the user record is enabled, one or more points of access the user may use to enable said user record, and one or more points of access the user may use to access the restricted area.

16. The method of claim 12, wherein the system operator associates one or more access parameters with a plurality of user records.

17. The method of claim 1, wherein the restricted area is an area of virtual space in a network.

18. The method of claim 1, further comprising:

   receiving, at the database, a system operator biometric sample;

   determining, at said system database, if the system operator biometric sample matches a system operator biometric record stored in the database; and

   if the system operator biometric sample matches a biometric record stored in the database, allowing the system operator access to present said portion of user information.

19. The method of claim 1, further comprising associating one or more managing privileges with said user record.

20. The method of claim 18, wherein said managing privileges include allowing the user to partially enable one or more other users to access the restricted area.

21. The method of claim 19, wherein the system operator must approve said partial enablement conducted by the user with managing privileges of one or more other users before allowing enablement.

22. The method of claim 1, further comprising:

    displaying, at the point of access, a portion of user information stored as said user record at the database;

    prompting the user to confirm said displayed information; and

    storing the confirmation presented by the user at the database.

23. The method of claim 21, wherein if a portion of said displayed information is incorrect, the user is provided with an opportunity to present the correct information.

24. The method of claim 1, wherein said point of access includes a record output device for outputting one or more records, the records being configured as one or more of a printed report, a media output to an electronic device, and an email.

25. The method of claim 23, wherein the record output includes one or more of the data entered during the system access, the data necessary to enable the user, the date of access, and the time of access.

26. The method of claim 1, wherein the system operator is provided with one or more of a record output of the user information stored in said system database and a record output of the identification code associated with said user record.

27. The method of claim 25, wherein said record output is configured as one or more of a printed report, a media output it an electronic device and an email.

28. The method of claim 26, wherein said record output is communicated to the user.

29. The method of claim 27, wherein said record output is communicated to the user automatically by the database.

30. A method for enabling a system operator to pre-enroll users within a system for biometric authentication, the method comprising:

    receiving, from the system operator, defined access rights for a user of the biometric authentication system;

    storing said defined access rights in association with an identification code as a partially enabled user record; and

    communicating said identification code to the user, said identification code

enabling said user to activate said user record through the provision of a biometric sample.

31. The method of claim 29, further comprising:

receiving, at a point of enablement, said identification code;

receiving, at the point of enablement, a user biometric sample;

determining if said identification code matches at least one identification code stored in the database;

if said identification code matches at least one identification code stored in the database, storing in the user record associated with said identification code the biometric sample; and

marking, said user record as active.

32. The method of claim 30, wherein said point of enablement is co-located with a point of allowance.

33. The method of claim 30, wherein the system operator can revoke said user record for any reason.

34. The method of claim 30, further comprising:

receiving, at the point of allowance, an activity request from the user; and

accepting said activity request if it meets the parameters associated with said user record.

35. The method of claim 33, wherein said activity request further comprises the user presenting a biometric sample and wherein that biometric sample is matched to a biometric record at the point of allowance.

36. The method of claim 33, wherein said activity request further comprises the user presenting a biometric sample and wherein that biometric sample is matched to a biometric record at a central location.

37. The method of claim 33, further comprising at least one biometrically authorized financial transaction.

38. The method of claim 30, further comprising:

receiving, at the point of allowance, an activity request from the user;

determining if said activity request meets the parameters stored in association with said user record;

if said activity request does not meet the parameters stored in association with said user record, initiating a system override;

notifying the system operator of said system override;

providing the system operator an opportunity to provide approval of said system override; and

accepting, at the point of allowance, said activity request if the system operator approves said initiated system override.

39. The method of claim 29, wherein said portion of the user information is pulled from a third party database.

40. A method for partially enabling a plurality of users to access a restricted area via biometric authentication, the method comprising:

receiving, at a system database in a biometric verification network, a plurality of portions of user information used to enable a plurality of users to access said area;

storing said portions of user information as a plurality of partially enabled user records;

generating, at the system database, a plurality of identification codes, each code uniquely associated with a user record selected from a plurality of user records; and

communicating said identification codes to the respective users.

41. The method of claim 39, further comprising:

receiving, at a system point of access, an identification code, said identification code presented by one of said plurality of users;

receiving at said system point of access, a biometric sample, said biometric sample presented by said one of said plurality of users;

storing, at the system database, said user biometric sample; and

marking said user record as enabled to access the system.

42. A method in a biometric system for enabling a user to access a restricted area, the method comprising:

pre-enrolling a user in the biometric system by storing a portion of a required amount of user record information in a database, said portion of required user record information including defined access rights to the restricted area;

receiving an enrollment completion request from the user, said enrollment completion request including an identification code associated with said user record and a user biometric sample;

storing said user biometric sample in said user record; and

marking said user record as an active user record.

43. The method of claim 41, further comprising generating said identification code and communicating said generated identification code to said user after pre-enrollment is complete.

44. A method in a biometric system for enabling a user to access a restricted area, the method comprising:

associating an identification code with an inactive user record, said inactive user record requiring input from a user for activation of said user record;

receiving an request from the user, said activation request including said identification code and biometric sample from the user; and

activating said user record upon storage of said biometric sample in said user record.

45. The method of claim 43, wherein said inactive user record includes access rights definitions.

46. A method for controlling access to a restricted area, the method comprising:

defining individual access rights to the restricted area for each of a plurality of users;

storing said defined individual access rights in a respective plurality of user records, each of the plurality of user records having a unique identification code associated therewith;

distributing said plurality of unique identification codes to said plurality of users;

identifying a user record upon receipt of an identification code from an activating

31

user; and

activating a user record associated with said identification code upon receipt of a biometric sample from said activating user, said activation permitting access to said active user to the restricted area in accordance with the defined access rights stored in said activated user record.